From: kim bruning
To: Microsoft ATR
Date: 1/23/02 5:18pm
Subject: Microsoft Settlement

Dear sir/madam,

I live in a small village called Wijk en Aalburg in the Netherlands. I am a software engineer, employed by a small computer company in Delft. Also, I study Biology in the city of Utrecht.

I am not a United States citizen, so I'm not sure how you will regard what I have to say. If I only comment on what I see then perhaps my opinions might still be of some value. I hope you will be able to use them.

Others have commented on many aspects of the settlement. Much of the text seems reasonable. I see two minor points which might need some improvement.

Point 1:

Under I.1. "All terms, including royalties [...] reasonable and non-discriminatory."

I would like to refer you to a discussion on RAND (Reasonable and non-Discriminatory) licensing as has been proposed for the world wide web consortium (The organization which sets standards for the world wide web).

http://www.w3.org/TR/2001/WD-patent-policy-20010816/

Note especially objections made by some of the w3c contributors. To wit: rand is not non-discriminatory. It discriminates directly against Open Source and Free Software projects. These projects simply cannot use or pay for such RAND licensing due to their legal structure. The arguments that could be made here are very similar to those stated in the w3c discussion. Here are some arguments of my own:

Royalty Free (RF) Licensing has been proposed as an alternative, and overcomes this weakness.

Why are Free Software and Open Source Software important? There are two arguments based on reason, and one is based on simple demonstration:

(1) The free software operating system Linux is considered by many to be a somewhat important competitor to Microsoft. It is distributed under the GNU general public licence (GPL) which is a distribution license. Allowing Microsoft to discriminate against such competitor would not be fair. It could also hardly be called non-discriminatory, of course.

reference: www.gnu.org

(2) As far as I know, original implementations of RFC 791 (Internet Protocol) and RFC 793 (Transmission Control Protocol) were released under the university of California's' "Berkeley Software Distribution" License. This is a free software license. These 2 protocols form the heart of the current day Internet. The implementation was left Royalty Free, and hence all parties adopted it. Also, since the original source was open, all parties could learn from it, and the TCP/IP system was quickly adopted worldwide. This is very important.

references:
IETF RFCs can be obtained from many sources. Here is one on the world wide web.:
http://www.ibiblio.org/pub/docs/rfc/rfc791.txt
http://www.ibiblio.org/pub/docs/rfc/rfc793.txt

(3) Quite simply put: The Simple Mail Transfer Protocol(RFC821) is royalty free, to the best of my knowledge. This protocol is used to transmit E-mail across the Internet. If it were not for SMTP, and if it were not for its royalty free status, I would not have been able to send this message.

http://www.ibiblio.org/pub/docs/rfc/rfc821.txt

A possible solution to the shortcoming in I.1. (and similar problems with related points under I) would be to allow for Royalty Free licensing of at very least the data interchange formats used by Microsoft.

As an aside:
Requiring Microsoft to submit their data formats (such as word and excel) to the International Standards Organization (ISO) might improve the situation further. Such standards organizations argue that good standardization has demonstrably improved economic gain, and stimulated competition between all parties concerned. I think that even Microsoft might actually gain from such an action in the long run. I see nothing wrong with this, because such gain would result from fair competition.

Reference:
www.iso.org

Point 2:

Under J it is said that Microsoft may not disclose information about security systems, and may set almost any requirement when sharing security information with a security vendor.

I am a programmer, not a certified computing security professional.

However, I have learnt much from such security professionals. I will try to summarize their point of view as best as I can. Please don't hold any minor errors or omissions I make against me. For a more comprehensive discussion of security, you could try looking at the scientific literature on this subject. Obtaining advice from a Data Encryption Scientist might be somewhat rewarding.

Open knowledge of algorithms and methods is a requirement for truly strong security. This seems reasonable to me. After all, if one knows of a certain weakness, one can compensate for it and prevent people from exploiting it.

If a hostile element was to be the only person to know a weakness in a security system, then that person would certainly be able to exploit that weakness. Further, security systems which are put up for public review can quickly be assessed for potential weaknesses, and these weaknesses can be repaired. No such process can be used for systems which are kept secret.

A second slight problem which some people have brought up is that there might be a weakness here. People might state "security concerns" as an excuse to sidestep what they are required to do under I in some situations. In fact this does not seem very hard to do from a technical perspective.

In short, section J on the whole might have some weaknesses. It might be a good idea to gain advice from one or more security experts (such as perhaps a professor teaching about data encryption, or people employed by a government security agency) to determine if this is indeed the case.

hopefully this is of some use to you,

sincerely,

Kim Bruning,
Anjelierstraat 47,
4261 CK Wijk en Aalburg,
The Netherlands.